

APPARATUS AND METHOD FOR MONITORING NETWORK

Patent Number: JP2002064492
Publication date: 2002-02-28
Inventor(s): OKADA HISASHI; HIROTA YOICHI; YAMAGISHI NORIKAZU; TAKESADA MUTSUHARU
Applicant(s): HITACHI ELECTRONICS SERVICE CO LTD
Requested Patent: ☐ JP2002064492
Application Number: JP20000247859 20000817
Priority Number(s):
IPC Classification: H04L12/24; H04L12/26; H04L12/28; H04L12/56; H04L29/14
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To provide a network monitor in which update of data is stopped depending on the data being taken in.

SOLUTION: A network monitoring computer 6 comprises a section 121 for taking in a packet on a network, and a section 122 for holding the packet. A data deciding section 14 makes a decision whether a packet acquired at the packet acquiring section 121 contains an IP address stored at an IP address storing section 13 and allotted to the network monitoring computer 6 or not. If that packet contains the IP address, a data acquisition control section 16 controls the operation such that packets being taken in subsequently are not written over a data storing section 122 and a communication control section 61 delivers Ping to other network monitoring computer stored at the IP address storing section 13.

Data supplied from the esp@cenet database - 12

(51) Int.Cl. ⁷	識別記号	F I	テマコード(参考)
H 0 4 L 12/24		H 0 4 L 11/08	5 K 0 3 0
12/26		11/00	3 1 0 Z 5 K 0 3 3
12/28		11/20	1 0 2 Z 5 K 0 3 5
12/56		13/00	3 1 3
29/14			
審査請求 有 請求項の数 8 O L (全 9 頁)			

(21) 出願番号 特願2000-247859(P2000-247859)

(22) 出願日 平成12年8月17日 (2000.8.17)

(71) 出願人 000233491

日立電子サービス株式会社
神奈川県横浜市戸塚区品濃町504番地2

(72) 発明者 岡田 尚志

神奈川県横浜市戸塚区品濃町504番地2
日立電子サービス株式会社内

(72) 発明者 廣田 陽一

神奈川県横浜市戸塚区品濃町504番地2
日立電子サービス株式会社内

(74) 代理人 100087170

弁理士 富田 和子 (外1名)

最終頁に続く

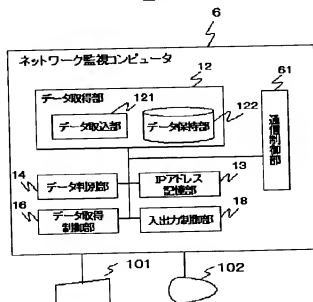
(54) 【発明の名称】 ネットワーク監視装置および方法

(57) 【要約】

【課題】 取り込んだデータに応じてデータの更新を停止するネットワーク監視装置の提供。

【解決手段】 ネットワーク監視コンピュータ6は、ネットワーク上のパケットを取り込むデータ取込部121と、パケットを保持するパケット保持部122とを備える。データ判別部14が、パケット取得部121が取り込んだパケットがIPアドレス記憶部13に記憶されたネットワーク監視コンピュータ6に割り振られたIPアドレスを含むかどうかを判別する。取り込んだパケットに前記IPアドレスが含まれる場合、データ取得制御部16はそれ以降に取り込むパケットをデータ保持部122に上書きしないように制御し、通信制御部61がIPアドレス記憶部13に記憶された他のネットワーク監視コンピュータにPingを送る。

図6



【特許請求の範囲】

【請求項1】 複数の情報処理装置が接続されたネットワークの監視を行うネットワーク監視装置において、前記ネットワークと接続されているときに、送信先装置の識別情報を少なくとも含む当該ネットワーク上のパケットを取り込んで、保持するパケット取得部と、当該ネットワーク監視装置を識別するための識別情報を記憶する記憶領域を有する識別情報記憶部と、前記パケット取得部が取り込んだパケットに含まれる前記送信先装置の識別情報が、前記識別情報記憶部に記憶された前記識別情報と一致するかどうかを判別する判別部と、

前記判別部における判別の結果、前記送信先装置の識別情報と前記識別情報記憶部に記憶された前記識別情報とが一致する場合、前記パケット取得部が前記パケットより後のパケットを保持しないように制御する制御部と、を備えることを特徴とするネットワーク監視装置。

【請求項2】 請求項1記載のネットワーク監視装置において、

前記パケット取得部は、

前記パケットを前記ネットワークから取り込み取り込み部と、

前記取り込み部が取り込んだパケットを保持する保持部と、を備え、

前記判別部における判別の結果、前記送信先装置の識別情報と前記識別情報記憶部に記憶された前記識別情報とが一致する場合、

前記制御部は、

前記取り込み部に前記パケットより後のパケットの取り込みを停止させることを特徴とするネットワーク監視装置。

【請求項3】 請求項1記載のネットワーク監視装置において、

前記パケット取得部は、

パケットを保持する保持部と、

前記パケットを前記ネットワークから取り込んで、前記保持部に書き込む取り込み部と、を備え、

前記制御部は、

前記判別部における判別の結果、前記送信先装置の識別情報と前記識別情報記憶部に記憶された前記識別情報とが一致する場合、

前記制御部は、

前記取り込み部が取り込んだ、前記パケットより後のパケットの前記保持部への書き込みを停止させることを特徴とするネットワーク監視装置。

【請求項4】 請求項1から3のうちのいずれか一項に記載のネットワーク監視装置において、

前記識別情報記憶部は、

他のネットワーク監視装置の識別情報を記憶する記憶領域をさらに有し、

当該ネットワーク監視装置は、

前記判別部における判別の結果、前記送信先装置の識別情報と前記識別情報記憶部に記憶された前記識別情報とが一致する場合、前記識別情報記憶部を参照して、前記他のネットワーク監視装置の識別情報を送信先装置の識別情報に設定したパケットを生成するパケット生成部と、

前記パケット生成部が生成したパケットを、前記ネットワークへ出力する出力部とを、さらに備えることを特徴とするネットワーク監視装置。

【請求項5】 請求項1から4のうちのいずれか一項に記載のネットワーク監視装置であって、

前記ネットワークの通信プロトコルは、TCP/IPであり、

前記ネットワーク上のパケットは、

少なくとも、当該パケットの送信先装置のIPアドレスを含み、

前記特定のパケットは、

当該パケットの送信先装置のIPアドレスに、特定のIPアドレスが設定されたpingコマンドのパケットであることを特徴とするネットワーク監視装置。

【請求項6】 複数の情報処理装置が接続されたネットワークと接続可能な情報処理装置において、

前記ネットワークと接続するための接続部と、

前記接続部が前記ネットワークと接続されているときに、送信先装置の識別情報を少なくとも含む当該ネットワーク上のパケットを取り込んで、保持するパケット取得部と、

当該情報処理装置を識別するための識別情報を記憶する記憶領域を有する識別情報記憶部と、

前記パケット取得部が取得したパケットに含まれる前記送信先装置の識別情報が、前記識別情報記憶部に記憶された前記識別情報と一致するかどうかを判別する判別部と、

前記判別部における判別の結果に応じて、当該パケットにより定まる情報に基づく処理を行う処理部と、

前記処理部が行う処理に伴って生じるエラーを検出するエラー検出部と、

前記エラー検出部がエラーを検出したとき、前記パケット取得部が前記パケットより後のパケットを保持しないように制御する制御部と、を備えることを特徴とする情報処理装置。

【請求項7】 記憶部を有するネットワーク監視装置におけるネットワーク監視方法であって、

当該ネットワーク監視装置を識別するための識別情報を前記記憶部に記憶し、

ネットワーク上のパケットを取り込み、前記記憶部に記憶されている識別情報が、当該取り込んだパケットに含まれるかどうかを判別し、

判別の結果、前記識別情報が前記パケットに含まれない

場合、前記取り込んだパケットを保持し、判別の結果、前記識別情報が前記パケットに含まれる場合、前記パケットより後のパケットは保持しないことを特徴とするネットワーク監視方法。

【請求項8】 記憶部を有するネットワーク監視装置に実行させるプログラムを記録した記録媒体であって、前記プログラムは、当該ネットワーク監視装置を識別するための識別情報を前記記憶部に記憶する処理と、ネットワーク上のパケットを取り込み、前記記憶部に記憶されている識別情報が、当該取り込んだパケットに含まれるかどうかを判別する処理と、判別の結果、前記識別情報が前記パケットに含まれない場合、前記取り込んだパケットを保持する処理と、判別の結果、前記識別情報が前記パケットに含まれる場合、前記パケットより後のパケットは保持しないように制御する処理と、を前記ネットワーク監視装置に実行させることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワーク監視技術にかかり、特にネットワークからのパケットの取り込みを制御する技術に関する。

【0002】

【従来の技術】 ネットワークトラブルの原因を解析するために、ネットワーク上のパケットを取り込んで、取り込んだパケットを保持するLANアナライザが広く用いられている。このパケットを保持するための記憶領域は容量が限られているので、サイクリックに利用される。したがって、一定時間が経過すると取り込んだパケットであっても上書きされて、消失する。

【0003】 また、従来のLANアナライザでは、例えば、プロトコルにTCP/IPを採用しているネットワークであれば、物理層、データリンク層、ネットワーク層、トランスポート層、セッション層でのプロトコルエラーを検出することができる。このエラーを検出すると、データの取得を停止して、その時点で記憶領域に保持されているデータが消失しないようにするストップリガー機能がある。

【0004】

【発明が解決しようとする課題】 しかしながら、通信の過程に原因があった場合でも、アプリケーション層などのデータにエラーが発生すると、LANアナライザはそのエラーを認識することができない。そのため、アプリケーション層などでエラーを検出してストップリガーをかけることもできない。したがって、この場合は、エラー発生時点の記憶領域のデータを保持し続けることが出来ないという問題点があった。

【0005】 本発明は、このような従来の問題点に着目

し、取り込んだデータに応じてデータの更新を停止するネットワーク監視技術を提供することを目的とする。

【0006】

【課題を解決するための手段】 前記目的を達成するため、本発明では識別情報を記憶する記憶部を備えたネットワーク監視装置が、以下の処理を行う。すなわち、当該ネットワーク監視装置を識別するための識別情報を記憶部に記憶する。ネットワーク上のパケットを取り込み、前記記憶部に記憶されている識別情報が、当該取り込んだパケットに含まれるかどうかを判別する。前記識別情報が前記パケットに含まれない場合、前記取り込んだパケットを保持する。前記識別情報が前記パケットに含まれる場合、前記パケットより後のパケットは保持しない。

【0007】

【発明の実施の形態】 以下、本発明の実施形態について、図面を用いて説明する。

【0008】 図1は、第1の実施形態が適用されるネットワークシステムの全体構成図である。すなわち、ネットワーク監視装置であるLANアナライザ1a、1bと、コンピュータ2a、2bと、テスト用コンピュータ3a、3bと、がLAN (Local Area Network) 8a、8bに接続されている。それぞれ同一構成のLAN 8a、8bがWAN (Wide Area Network) 9で接続されている。このネットワークシステムは、通信プロトコルにTCP/IPを用いている。ただし、通信プロトコルはTCP/IPに限定されない。たとえば、他の通信プロトコルを用いてもよいし、IP (インターネットプロトコル) と、TCP (トランスミッションコントロールプロトコル) 以外の上位プロトコルとを組み合わせてもよい。

【0009】 本実施の形態では、コンピュータ2a、2bが、あらかじめ定められた事象の発生を検出して、それをLANアナライザ1a、1bが検知可能な事象に変換を行う。具体的には、コンピュータ2a、2bが、アプリケーション層でのエラー等を検出すると、ネットワーク上にあるすべてのコンピュータにとって、論理的に存在しないIPアドレス (新規に割り当てられたIPアドレス) に対するpingコマンドの発行という事象に変換する。

【0010】 LANアナライザ1は、ネットワークのトラブル発生時に設置され、LAN 8上のパケットを取り込んで保持する。ネットワークの保守担当者は、LANアナライザに保持されたパケットを解析して、トラブルの原因の究明に役立てる。LANアナライザ1の詳細な構成は図4(a)を用いて説明する。

【0011】 LANアナライザ1は、図4(a)に示すように、キーボード等の入力装置101およびCRT、液晶ディスプレイ等の表示装置102が接続されている。LANアナライザ1は、データ取得部12と、IP

アドレス記憶部13と、データ判別部14と、データ取得制御部16と、表示制御部18とを、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。

【0012】データ取得部12は、データ取込部121とデータ保持部122とを有する。データ取込部121は、LAN上のパケットを取り込む。取り込んだパケットは、図示しないバッファに一時的に記憶される。

【0013】データ保持部122は、データ取込部121が取り込んだパケットを保持する。データ保持部122は、例えば、一定の容量を持つサイクリックバッファで構成される。つまり、例えば100メガバイト程度の容量を持ち、パケットを順次記憶していき、全領域にデータが記憶された状態になると、時間的に最も古いデータに上書きして記憶していく。

【0014】IPアドレス記憶部13は、LANアナライザ1と同じLAN8に接続されているテスト用コンピュータ3に設定されたIPアドレス80を記憶する領域を備える。例えば、LANアナライザ1aのIPアドレス記憶部13には、テスト用コンピュータ3aのIPアドレス80c(***.***.34.56)が記憶される。

【0015】データ判別部14は、データ取込部12が取り込んだパケットが特定のパケットであるかどうかを判別する。例えば、取り込んだパケットの送信先のIPアドレスがIPアドレス記憶部13に記憶されているIPアドレスと一致するかどうかを判別する。具体的には、LANアナライザ1aでは、取り込んだパケットの送信先IPアドレスが、IPアドレス80c(***.***.34.56)であるかどうかを判別する。さらに好ましくは、取り込んだパケットがPingコマンドであるかどうかを併せて判別してもよい。

【0016】判別の結果、特定のパケットである場合は、その旨をデータ取得制御部16へ通知する。特定のパケットでない場合は、データ取込部121に対して、図示しないバッファに記憶されているパケットをデータ保持部122へ書き込むように指示する。

【0017】データ取得制御部16は、データ取得部12が行うデータ取得を制御する。例えば、データ判別部14からの通知を受けて、データ取得部12に対して、特定のパケットより後のパケットを保持しないように指示する。好ましくは、前記特定のパケットより後にLAN上を伝送されてくるパケットについては、データ取込部121が取り込まないように制限するようにしてもよい。あるいは、前記特定のパケットより後にLAN上を伝送されてくるデータ取込部121が取り込んだパケットについては、図示しないバッファからデータ保持部122へ書き込まないようにしてもよい。

【0018】こうすることで、特定のパケットを受信した以降、データ保持部122の記憶内容が更新されて、

書きかえられてしまうことを回避できる。その結果、特定のパケットを受信する直前にネットワーク上に存在したパケットが上書きされずに、保持しつづけることができる。

【0019】入出力制御部18は、入力装置10および表示装置102の制御を行う。例えば、入力装置10から入力を受け付け、表示装置102にデータ保持部122に保持しているデータを表示させる。

【0020】コンピュータ2aとコンピュータ2bには、それぞれIPアドレス80a、80bが割り振られていて、相互に通信を行い、所定のアプリケーションを実行する。コンピュータ2の詳細な構成は、図4(b)を用いて説明する。図4(b)に示すように、コンピュータ2は、通信制御部21と、1以上のデータ処理部22と、データ処理部22でのエラー発生を検出するエラー検出部23と、IPアドレス記憶部24を、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。

【0021】通信制御部21は、ネットワーク上の他の装置との通信を制御する。例えば、LAN8上のパケットを取得し、自コンピュータ2宛てのパケットを受け付ける。また、ネットワーク上の他の装置へ送信するために、パケットを生成して、LAN8へ出力する。

【0022】データ処理部22は、通信制御部21が受け付けたパケットが示す情報に基づいて、ユーザが定義した所定のアプリケーション処理を行う。

【0023】エラー検出部23は、データ処理部22であらかじめ定められた事象が発生したかどうかを監視し、当該事象が発生すると、それをエラーとして検出する。エラー検出部23が検出すべき事象は、ユーザが任意に指定することができる。たとえば、データ処理部22における処理の異常終了、他の装置との通信処理におけるタイムアウト等の通信不良、プロトコルの上位階層でのエラー等を検出するようにしてもよい。さらに好ましくは、いわゆる警告のような軽微な不具合もエラーとして検出するようにしてもよい。

【0024】さらに、エラー検出部23は、エラーを検出すると、IPアドレス記憶部24に記憶されているIPアドレスの装置に対してエラー検出を通知する。例えば、IPアドレス記憶部24に記憶されているIPアドレスへ宛てて、Pingコマンドを発行するように通信制御部21へ指示する。

【0025】IPアドレス記憶部24は、LANアナライザ1と同じLAN8に接続されているテスト用コンピュータ3に設定されたIPアドレス80、および、WAN9を介して接続される他のLAN8に接続されているテスト用コンピュータ3に設定されたIPアドレス80を記憶する。例えば、コンピュータ2a、2bのいずれのIPアドレス記憶部24にも、テスト用コンピュータ

3a、3bのIPアドレス80c(***.***.34.56)および80d(***.***.12.78)が記憶される。

【0026】テスト用コンピュータ3a、bは、ネットワークトラブルの解析用に設置されるコンピュータである。したがって、通常時には設置する必要はない。各テスト用コンピュータ3a、bには、それぞれIPアドレス80c、80dが割り振られている。テスト用コンピュータ3は、IPアドレスを割り振って、LAN8に接続できる装置であれば、なんでもよい。

【0027】本実施形態での処理手順について、図7を用いて説明する。

【0028】図7は、LANアナライザ1aの処理手順を示したものである。LANアナライザ1bについては、LAN8aとLAN8bが異なる点以外は同様である。

【0029】入力装置101から所定の指示を受けて、データ取込121がデータの取り込みを開始する(S101)。取り込んだパケットがテスト用コンピュータ3a宛てのものであるかどうかを判別する(S102)。テスト用コンピュータ3a宛てでない場合には、そのパケットをデータ保持部122に書き込んで保持する(S103)。その後、S101へ戻って処理を繰り返す。これにより、コンピュータ2a、2b間の通信を含む、LAN8a上のパケットが保持されていく。

【0030】このとき、例えば、コンピュータ2bのデータ処理部22でエラーが発生したとする。すると、コンピュータ2bのエラー検出部23がエラーを検出する。そして、コンピュータ2bからテスト用コンピュータ3a、3bに宛ててPingコマンドが発行される。

【0031】LANアナライザ1aが、テスト用コンピュータ3a宛てのパケットを取り込むと(S101、S102)、データ取得制御部16が、そのパケットより後にLAN8a上を伝送されてくるパケットの取得を禁止する(S104)。これにより、データ保持部122が更新されない。つまり、テスト用コンピュータ3a宛てのパケットを取得した時点でデータ保持部122に記憶されているパケットが、そのまま保持される。

【0032】つぎに、本発明の第2の実施形態が適用されるネットワークシステムの全体構成を図2に示す。すなわち、ネットワーク監視装置であるLANアナライザ1と、コンピュータ2と、テスト用コンピュータ3と、がLAN8に接続されている。監視コンピュータ5がLAN8bに接続され、LAN8a、bがWAN9で接続されている。なお、以下の実施形態において、第1の実施形態と同一の構成には同一の符号を付して説明を省略する場合がある。

【0033】本実施形態で用いるLANアナライザ1、コンピュータ2、テスト用コンピュータ3の構成は、第1の実施形態と同様である。

【0034】監視コンピュータ5は、コンピュータ2の

状態を監視する。監視コンピュータ5の構成は図5に示すように、通信制御部51と、監視制御部52と、IPアドレス記憶部53とを、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。

【0035】通信制御部51は、ネットワーク上の他の装置との通信を制御する。例えば、LAN8上のパケットを取得し、自監視コンピュータ5宛てのバケットを受け付ける。また、ネットワーク上の他の装置へ送信するために、パケットを生成して、LAN8へ出力する。

【0036】監視制御部52は、コンピュータ2の動作状態を監視する。例えば、定期的にコンピュータ2に対してメッセージを出力し、応答があるかどうかを確認する。応答がない場合、コンピュータ2に何等かの異常があるとみなして、テスト用コンピュータ3へその旨を通知する。具体的には、定期的にコンピュータ2宛てのPingコマンドを出力するように通信制御部51へ指示する。このPingに対する応答を通信制御部51を介して受け付ける。一定時間内に応答がない場合、テスト用コンピュータ3へPingコマンドを出力するように通信制御部51へ指示する。

【0037】IPアドレス記憶部53は、少なくとも、コンピュータ21と、テスト用コンピュータ3に設定されたIPアドレス80a、80cを記憶する。

【0038】本実施形態における監視コンピュータ5の処理手順について説明する。LANアナライザ1の処理手順は、図7と同様である。

【0039】コンピュータ2が図示しない他の装置等と通信をしながら、所定の処理を行っている。このときに、監視コンピュータ5は、コンピュータ2に対して定期的にPingコマンドを送り、その応答を確認する(S201、S202)。所定時間内に応答がない場合等、異常を検出した場合、監視コンピュータ5はテスト用コンピュータ3へPingを発行する(S203)。

【0040】このテスト用コンピュータ3宛てのPingを受け取ったLANアナライザ1は、図7のフローにしたがって動作する。

【0041】第1の実施形態では、コンピュータ2が自らエラーを検出してテストコンピュータ3宛てのPingを発行した。このため、コンピュータ2がハングアップまたはダウンして、自らPingを発行することができないような場合は、エラーを検出することができなかった。しかし、本実施形態では、そのような場合もエラーを検出することができる。

【0042】さらに、第1の実施形態では、コンピュータ2の内部にエラー検出部23を設ける必要がある。しかし、現実には、コンピュータ2内部にエラー検出部を設けたくない場合もある。そのような場合に、本実施形態のような構成にすれば、コンピュータ2には手を加えることなく、監視コンピュータ5をネットワークに追加

するだけで、同様の機能を実現することができる。

【0043】つぎに、本発明の第3の実施形態が適用されるネットワークシステムの全体構成図を図3に示す。すなわち、コンピュータ2a、2bと、ネットワーク監視装置コンピュータ6a、6bとが、LAN8a、8bに接続されている。それぞれ同一構成のLAN8a、8bがWAN9で接続されている。ネットワーク監視コンピュータ6a、6bには、それぞれ、IPアドレス80e、80fが割り振られている。

【0044】本実施形態で用いるコンピュータ2a、2bの構成は、第1の実施形態と同様である。ネットワーク監視コンピュータ6a、6bの構成を図6に示す。

【0045】ネットワーク監視コンピュータ6は、図6に示すように、キーボード等の入力装置101、および、CRT、液晶ディスプレイ等の表示装置102が接続されている。ネットワーク監視コンピュータ6は、通信制御部61、データ取得部12と、IPアドレス記憶部13と、データ判別部14と、データ取得制御部16と、表示制御部18とを、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。

【0046】通信制御部61は、ネットワーク上の他の装置との通信を制御する。例えば、ネットワーク上の他の装置へ送信するために、パケットを生成して、LAN8へ出力する。具体的には、ネットワーク監視コンピュータ6aであれば、データ判別部14から通知を受けると、IPアドレス記憶部13からネットワーク監視コンピュータ6bのIPアドレス80fを取得して、Pingを送る。

【0047】IPアドレス記憶部13には、自ネットワーク監視コンピュータ6に割り当てられたIPアドレス80と、他のLAN8に接続されているネットワーク監視コンピュータ6に割り当てられたIPアドレス80とを記憶する領域を備える。例えば、ネットワーク監視コンピュータ6aであれば、自コンピュータ6用の領域にIPアドレス80e(***.***.34.78)を記憶し、他のネットワーク監視コンピュータの領域にIPアドレス80f(***.***.12.89)を記憶している。

【0048】データ判別部14は、取り込んだパケットの送信先のIPアドレスが、IPアドレス記憶部13の自装置用IPアドレス記憶領域に記憶されているIPアドレスと一致するかどうかを判別する。つまり、ネットワーク監視コンピュータ6aでは、取り込んだパケットの送信先IPアドレスが、IPアドレス80e(***.***.12.89)であるかどうかを判別する。判別の結果、一致する場合は、その旨を通信制御部61およびデータ取得制御部16へ通知する。

【0049】本実施形態のネットワーク監視コンピュータ6には、IPアドレスが割り振られているので、他の

実施形態と異なり、テスト用コンピュータ3を備える必要がない。つまり、自コンピュータ6宛てのパケットを受信すると、データ保持部122が更新されない。これにより、自コンピュータ6宛てのパケットを取得した時点でデータ保持部122に記憶されているパケットが、そのまま保持される。

【0050】さらに、ネットワーク上の他の装置に対してパケットを送出することができるので、コンピュータ2は、同一LAN8上のネットワーク監視コンピュータ6に対してエラー検出を通知するPingを送ればよい。

【0051】なお、第1の実施形態において、LANアナライザ1とコンピュータ2を一体として構成することもできるし、第3の実施形態において、ネットワーク監視コンピュータ6とコンピュータ2を一体として構成してもよい。また、上記実施形態において説明した各構成は、可能な限り組み合わせの変更、追加、省略等を行うことができる。

【0052】さらに、上記いずれの実施形態においても、WAN9により接続される2つのLAN8a、8bを用いて説明したが、LAN8の数はこれ以上であっても同様である。

【0053】

【発明の効果】本発明によれば、ネットワーク監視装置が取り込んだデータに応じて、保持しているデータの更新しないようにすることができる。

【図面の簡単な説明】

【図1】本発明が適用される第一の実施形態におけるネットワークシステムの全体構成図である。

【図2】本発明が適用される第二の実施形態におけるネットワークシステムの全体構成図である。

【図3】本発明が適用される第三の実施形態におけるネットワークシステムの全体構成図である。

【図4】(a)は、本発明にかかる実施形態におけるLANアナライザの構成を説明する説明図であり、(b)は、本発明にかかる実施形態におけるコンピュータの構成を示す説明図である。

【図5】本発明にかかる実施形態における監視コンピュータの構成を示す説明図である。

【図6】本発明にかかる実施形態におけるネットワーク監視コンピュータの構成を示す説明図である。

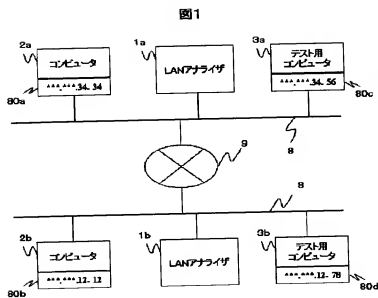
【図7】本発明にかかるLANアナライザの処理手順を示すフローチャートである。

【図8】本発明にかかる監視コンピュータの処理手順を示すフローチャートである。

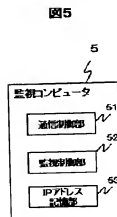
【符号の説明】

1…LANアナライザ、2…コンピュータ、3…テスト用コンピュータ、5…監視コンピュータ、6…ネットワーク監視コンピュータ、8…LAN、9…WAN。

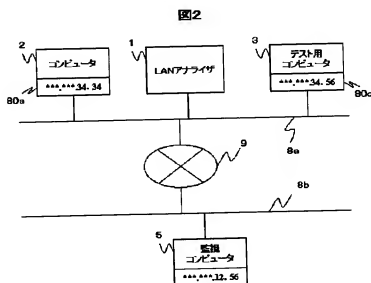
【図1】



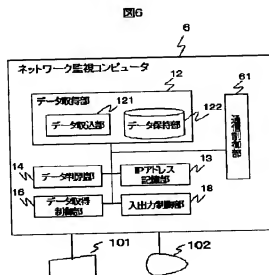
【図5】



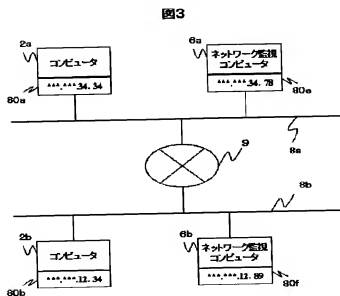
【図2】



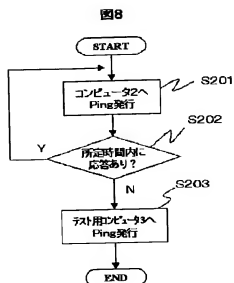
【図6】



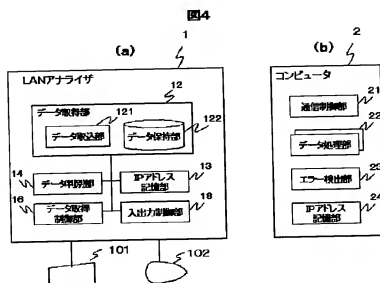
【図3】



【図8】

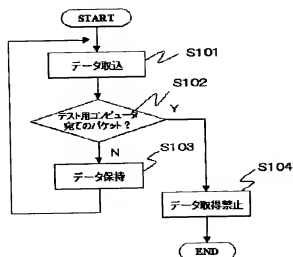


【図4】



【図7】

図7



フロントページの続き

(72)発明者 山岸 令和
神奈川県横浜市戸塚区品濃町504番地2
日立電子サービス株式会社内
(72)発明者 武貞 睦治
神奈川県横浜市戸塚区品濃町504番地2
日立電子サービス株式会社内

Fターム(参考) 5K030 GA11 GA17 HB28 HB29 HC01
HC14 HD06 JA10 KA04 KA06
5K033 AA03 AA04 CC01 DA01 DA06
DB20 EA03
5K035 AA02 AA04 KK01